In the claims:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (currently amended) [[The]] A method for mutual authentication of a first station and a second station, comprising:

~~encrypting~~ providing a particular data random key at the first station, disassembling and ~~by first~~ veiling the particular data random key [[using]] by forming a first conversion array seeded by a shared secret and then encrypting the first conversion array ~~veiled particular data random key~~ to produce a first encrypted data set [[key]], where access to the shared secret indicates authenticity of the first station;

sending a first message to the second station including the first encrypted data set [[key]], where the second station decrypts first encrypted data set and unveils and reassembles said particular data random key using the shared secret, and where the second station disassembles and veils ~~encrypts the particular data random key by first veiling~~ a version of the particular data random key [[using]] by forming a second conversion array seeded by the shared secret and then ~~encrypting~~ encrypts the ~~veiled~~ second conversion array ~~version of the particular data random key~~ to produce a second encrypted key, and sends a second message to the first station carrying the second encrypted data set [[key]], where access to the shared secret indicates authenticity of the second station; [[and]]

receiving the second message, and decrypting the second encrypted data set, and reassembling and unveiling the version of the particular data random key at the first station; and

determining at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so providing an additional particular data random key at the first station, disassembling and veiling the additional particular data random key by forming a third conversion array seeded by an additional shared secret and then encrypting the third conversion array to produce a first additional encrypted data set, where access to the additional shared secret indicates authenticity of the first station;

sending a third message to the second station including the first additional encrypted data set, where the second station decrypts the first additional encrypted data set and reassembles and unveils said additional particular data random key using the additional shared secret, and where

the second station disassembles and veils a version of the additional particular data random key by forming a fourth conversion array seeded by the additional shared secret and then encrypts the fourth conversion array to produce a second additional encrypted data set, and sends a fourth message to the first station carrying the second additional encrypted data set, where access to the additional shared secret indicates authenticity of the second station; and

receiving the fourth message, and decrypting the second additional encrypted data set and reassembling and unveiling the version of the additional particular data random key at the first station, and

determining at the first station if the version of the additional data random key matches an expected version the additional data random key, and if so continuing with further exchanges of messages with the second station.

2. (canceled).

3. (currently amended) The method of claim 1 [[2]], wherein said additional particular data random key is the same as the particular data random key.

4. (currently amended) The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including ~~instructions~~

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

placing a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

5. (withdrawn) The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values

corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

placing a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

6. (withdrawn) The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

7. (withdrawn) The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

8. (currently amended) The method of claim 1, including presenting a [[use]] user interface to the second station from the first station carrying parameters of said first and second conversion arrays.

9. (original) The method of claim 1, including executing an interactive exchange of messages to deliver the particular data random key from the first station to the second station.

10. (currently amended) A data processing apparatus, comprising:

a processor, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to ~~encrypt~~ provide a particular data random key at the first station and to disassemble and veil ~~by first veiling~~ the particular data random key [[using]] by forming a first conversion array seeded by a shared secret and then to encrypt the first conversion array ~~veiled particular data random key~~ to produce a first encrypted data set ~~key~~, where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted data set [[key]], where the second station decrypts and unveils the first encrypted data set ~~said particular data random key~~ using the shared secret, and where the second station ~~encrypts the particular data random key by first veiling~~ disassembles and veils a version of the particular data random key ~~using~~ by forming a second conversion array seeded by the shared secret and then to encrypt ~~encrypting~~ the ~~veiled version of the particular data random key~~ second conversion array to produce a second encrypted data set [[key]], and sends a second message to the first station carrying the second encrypted data set [[key]], where access to the shared secret indicates authenticity of the second station; [[and]]

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station; and

logic to determine at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so provide an additional particular data random key at the first station, disassemble and veil the additional particular data random key by forming a third conversion array seeded by an additional shared secret and then to encrypt the third conversion array to produce a first additional encrypted data set, where access to the additional shared secret indicates authenticity of the first station;

logic to send a third message to the second station including the first additional encrypted data set, where the second station decrypts the first additional encrypted data set and reassembles and unveils the additional particular data random key using the additional shared secret, and where the second station disassembles and veils a version of the additional particular data random key by forming a fourth conversion array seeded by the additional shared secret and then encrypts the fourth conversion array to produce a second additional encrypted data set, and sends a fourth message to the first station carrying the second additional encrypted data set, where access to the additional shared secret indicates authenticity of the second station;

logic to receive the fourth message, and decrypt the second additional encrypted data set and to reassemble and unveil the version of the additional particular data random key at the first station; and

logic to determine at the first station if the version of the additional data random key matches an expected version the additional data random key, and if so to continue with further exchanges of messages with the second station.

11. (canceled).

12. (currently amended) The apparatus of claim 10 [[11]], wherein said additional particular data random key is the same as the particular data random key.

13. (original) The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

to place a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

14. (withdrawn) The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

to place a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

15. (withdrawn) The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

16. (withdrawn) The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

17. (original) The apparatus of claim 10, including logic to present a user interface to the second station from the first station carrying parameters of said first and second conversion arrays.

18. (original) The apparatus of claim 10, including logic to execute an interactive exchange of messages to deliver the particular data random key from the first station to the second station.

19. (currently amended) An article, comprising:

machine readable data storage medium having computer program instructions stored therein for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, said instructions comprising

logic to ~~encrypt~~ provide a particular data random key at the first station and to disassemble and veil ~~by first veiling~~ the particular data random key ~~using~~ by forming a first conversion array seeded by a shared secret and then to encrypt the first conversion array ~~veiled particular data random key~~ to produce a first encrypted data set [[key]], where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted data set ~~key~~, where the second station decrypts and unveils the first encrypted data set ~~said particular data random key~~ using the shared secret, and where the second station ~~encrypts the particular data random key by first veiling~~ disassembles and veils a version of the particular data random key ~~using~~ by forming a second conversion array seeded by the shared secret and then to encrypt ~~encrypting~~ the ~~veiled version of the particular data random key~~ second conversion array to produce a second encrypted data set [[key]], and sends a second message to the first station carrying the second encrypted data set [[key]], where access to the shared secret indicates authenticity of the second station; [[and]]

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station; and

logic to determine at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so provide an additional particular data random key at the first station, disassemble and veil the additional particular data random key by forming a third conversion array seeded by an additional shared secret and then to encrypt the third conversion array to produce a first additional encrypted data set, where access to the additional shared secret indicates authenticity of the first station;

logic to send a third message to the second station including the first additional encrypted data set, where the second station decrypts the first additional encrypted data set and reassembles and unveils the additional particular data random key using the additional shared secret, and where the second station disassembles and veils a version of the additional particular data random key by forming a fourth conversion array seeded by the additional shared secret and then encrypts the fourth conversion array to produce a second additional encrypted data set, and sends a fourth message to the first station carrying the second additional encrypted data set, where access to the additional shared secret indicates authenticity of the second station;

logic to receive the fourth message, and decrypt the second additional encrypted data set and to reassemble and unveil the version of the additional particular data random key at the first station; and

logic to determine at the first station if the version of the additional data random key matches an expected version the additional data random key, and if so to continue with further exchanges of messages with the second station.

20. (canceled).

21. (original) The article of claim 19, wherein said additional particular data random key is the same as the particular data random key.

22. (original) The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

to place a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

23. (withdrawn) The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

to place a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

24. (withdrawn) The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values

corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

25. (withdrawn) The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

26. (original) The article of claim 19, wherein the instructions include logic to present a user interface to the second station from the first station carrying parameters of said first and second conversion arrays.

27. (original) The article of claim 19, wherein the instructions include logic to execute an interactive exchange of messages to deliver the particular data random key from the first station to the second station.

28. (new) A method for mutual authentication of a first station and a second station, comprising:

providing a particular data random key at the first station, disassembling and veiling the particular data random key by forming a first conversion array seeded by a shared secret and then encrypting the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station;

sending a first message to the second station including the first encrypted data set ~~key~~, where the second station decrypts first encrypted data set and unveils and reassembles said particular data random key using the shared secret, and where the second station disassembles and veils a version of the particular data random key by forming a second conversion array seeded by the shared secret and then encrypts the second conversion array to produce a second encrypted key, and sends a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

receiving the second message, and decrypting the second encrypted data set, and reassembling and unveiling the version of the particular data random key at the first station; and

determining at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so continuing with further exchanges of messages with the second station;

where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

placing a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

29. (new) A data processing apparatus, comprising:

a processor, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to provide a particular data random key at the first station and to disassemble and veil the particular data random key by forming a first conversion array seeded by a shared secret and then to encrypt the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted data set ~~key~~, where the second station decrypts and unveils the first encrypted data set using the shared secret, and where the second station disassembles and veils a version of the particular data random key by forming a second conversion array seeded by the shared secret and then to encrypt the second conversion array to produce a second encrypted data set, and sends a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station; and

logic to determine at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so to continue with further exchanges of messages with the second station;

where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

to place a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

30. (new) An article, comprising:

machine readable data storage medium having computer program instructions stored therein for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, said instructions comprising

logic to provide a particular data random key at the first station and to disassemble and veil the particular data random key by forming a first conversion array seeded by a shared secret and then to encrypt the first conversion array to produce a first encrypted data set, where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted data set ~~key~~, where the second station decrypts and unveils the first encrypted data set using the shared secret, and where the second station disassembles and veils a version of the particular data random key by forming a second conversion array seeded by the shared secret and then to encrypt the second conversion array to produce a second encrypted data set, and sends a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station; and

logic to determine at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so to continue with further exchanges of messages with the second station;

where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

to place a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

31. (new) A method for mutual authentication of a first station and a second station, comprising:

providing a particular data random key at the first station, disassembling and veiling the particular data random key by forming a first conversion array seeded by a shared secret and then encrypting the first conversion array to produce a first encrypted data set ~~key~~, where access to the shared secret indicates authenticity of the first station;

sending a first message to the second station including the first encrypted data set, where the second station decrypts first encrypted data set and unveils and reassembles said particular data random key using the shared secret;

receiving the first message at the second station and decrypting the first encrypted data set, and reassembling and unveiling the particular data random key at the second station; and

determining at the second station if the particular data random key matches an expected version the particular data random key, and if so and disassembling and veiling a version of the particular data random key by forming a second conversion array seeded by the shared secret and then encrypting the second conversion array to produce a second encrypted key, and sending a second message to the first station carrying the second encrypted data set, where access to the shared secret indicates authenticity of the second station;

receiving the second message at the first station, and decrypting the second encrypted data set, and reassembling and unveiling the version of the particular data random key at the first station; and

determining at the first station if the version of the particular data random key matches an expected version the particular data random key, and if so providing an additional particular data random key at the first station, disassembling and veiling the additional particular data random key by forming a third conversion array seeded by an additional shared secret and then encrypting the third conversion array to produce a first additional encrypted data set, where access to the additional shared secret indicates authenticity of the first station;

sending a third message to the second station including the first additional encrypted data set;

receiving the third message at the second station and decrypting the first additional encrypted data set and unveiling and reassembling the additional particular data random key using the additional shared secret, and determining at the second station if the additional particular data random key matches an expected version the additional particular data random

key, and if so disassembling and veiling a version of the additional particular data random key by forming a fourth conversion array seeded by the additional shared secret and then encrypting the fourth conversion array to produce a second additional encrypted data set;

sending a fourth message to the first station carrying the second additional encrypted data set, where access to the additional shared secret indicates authenticity of the second station;

receiving the fourth message, and decrypting the second additional encrypted data set and unveiling and reassembling the version of the additional particular data random key at the first station; and

determining at the first station if the version of the additional data random key matches an expected version the additional data random key, and if so continuing with further exchanges of messages with the second station.

///